V210 Series

PCI PTS POI v6.1 Security Policy

Rev 2.13 – 18 October 2022

Contents

PURPOSE

- This Security Policy provides guidance for the proper and secure usage of the PCI PTS POI v6.0 approved V210 payment terminal series including information on key-management responsibilities, administrative responsibilities, device functionality, identification, and environmental requirements.
- The V210 series is comprised of four models: V210 M1, V210 4G, V210 4G ONLY, and the V210 4G PLUS.
- Any deviation from the approved use of the device will invalidate the PCI PTS POI v6.0 approval.

GENERAL DESCRIPTION

PRODUCT NAME AND APPEARANCE

- Figures 1 and 2 show the V210 terminal appearance. The standard color for the terminal is black, but it may be offered in distinct colors and support the customer's branding. Different keypad legends are provided according to local requirements.
- The product name is visible on the label at the back side of the device; see Figure 3.

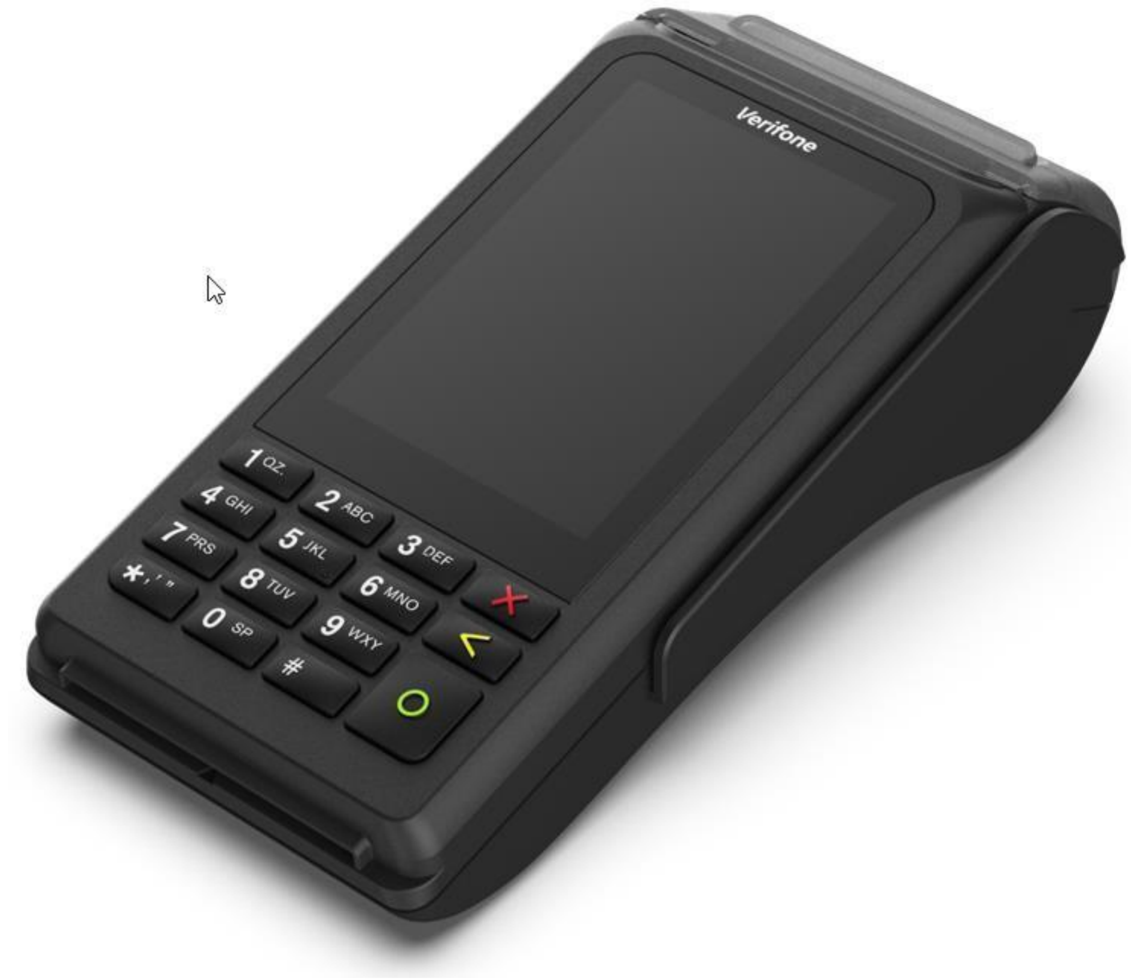


Figure 1, Front views of
V210 M1, V210 4G, V210 4G ONLY, V210 4G PLUS

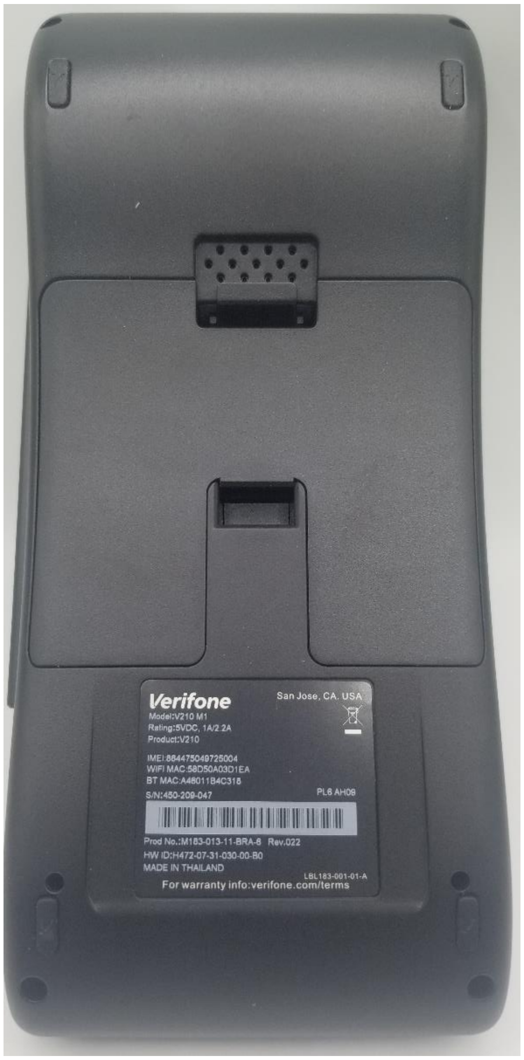


Figure 2, An Example of V210 Series Devices Rear view

PRODUCT TYPE

- V210 terminals are integrated handheld Point-of-Interaction (POI) devices designed to process online and offline transactions in an attended or semi-attended environment. The terminal is PCI PTS version 6 approved as a PED class of device and is equipped with:
    - A variety of payment methods including: EMV chip and PIN, chip and signature, magnetic- stripe and contactless.
    - CAT-M1 cellular modem for Brazil and Latin American Countries (LAC) and a 4G Cat1 for the rest of the world.

- Bluetooth, Wi-Fi, GPS, USB host and device, one SIM + one SIM/SAM (Secure Access Module) slot.
- Support for transmit-only Bluetooth beacons (iBeacon and Eddystone). Over the Air (OTA) provisioning is not allowed.
- Interface to support charging and expanded communications via a full-featured base module, also referred to as a docking station.

IDENTIFICATION

- The product model name and hardware version (HW ID) is printed on the label at the back side of the device; see Figure 3. The label should not be torn off, covered, or manipulated in any way.
- Hardware version number includes variable fields for designating product options; see Table 1.
- Please note: Positions 5, 8, 11, 15, 18 in the table below, are just field separators (-).

Hardware version variable positions																					
Fixed	Variable	H	4	7	2	-	0	7	-	C	C	-	0	x	x	-	x	0	-	B	R
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1		HW ID Part Number Key: • “H”																			
2,3,4		Model: • “472”: For V210m																			
6,7		Card-reader options: “07”: CTLS, ICCR, MSR Legend: • Bit 0: MSR • Bit 1: ICCR • Bit 2: CTLS • Bit 3: Hybrid • Bit 4: 2nd MSR • Bit 5: RFU																			

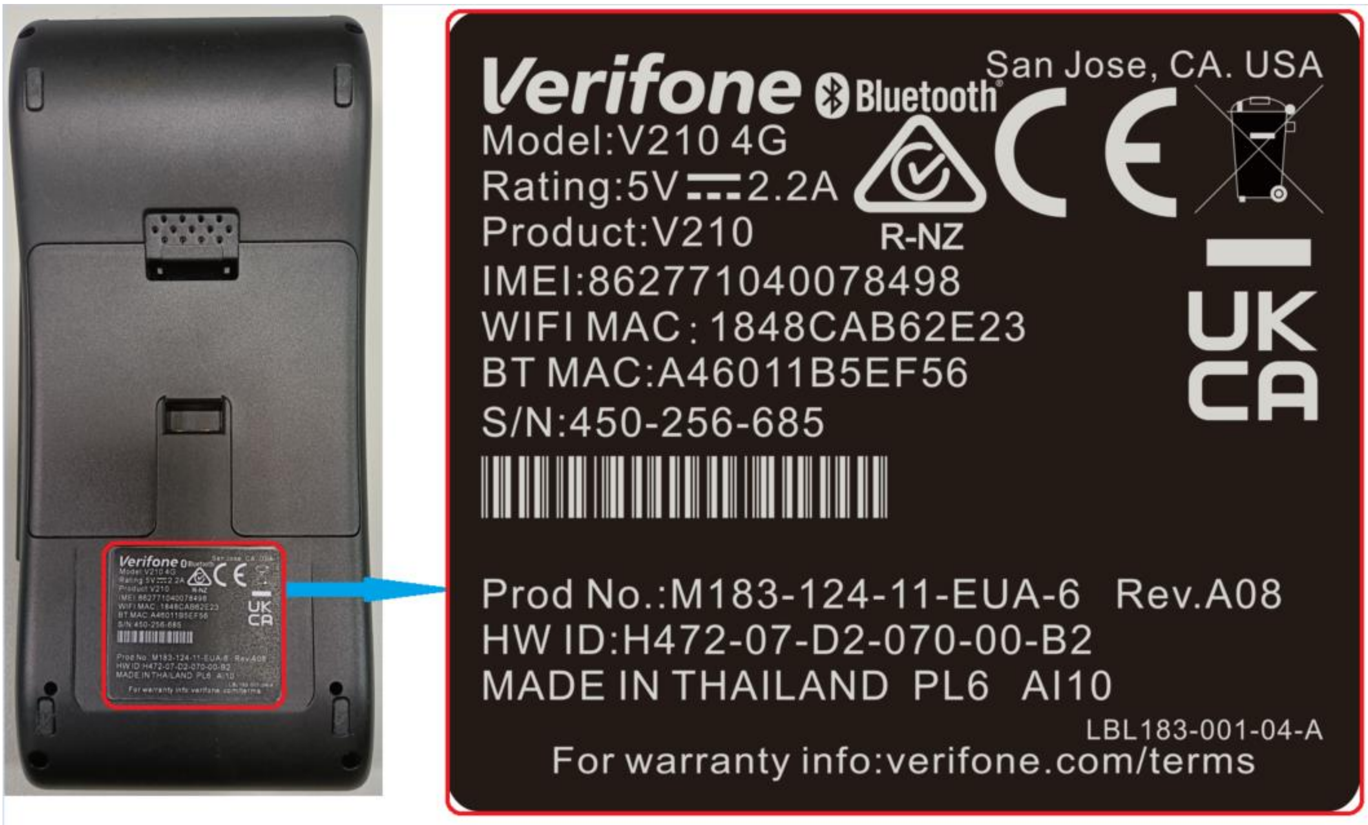
		• Bit 6: RFU • Bit 7: RFU
9,10		Range of Communication options. The only permitted values for “CC” are: • “31” = V210 M1: Cat-M1; Single Band Wi-Fi; BT • “91” = V210 M1: Cat-M1; Dual Band Wi-Fi; BT • “D2” = V210 4G: 4G LTE-Cat1; Dual Band Wi-Fi; Ethernet • “D2” = V210 4G PLUS: 4G LTE-Cat1; Dual Band Wi-Fi; Ethernet;Extended-PLUS Memory • “40” = V210 4G ONLY 4G LTE-Cat1 • “42” = V210 4G ONLY 4G LTE-Cat1; Ethernet
12		Physical Privacy Shield options • “0”: No Privacy Shield
	13	Keypad artwork. • 'N': No keypad • ‘3’: Standard • ‘4’: Holland • '6': Arabic • '7': EBS100 • '8': Sweden / Numeric • '9': RNIB • 'X': UMS/ICBC • 'K': Korea • 'S': Stone (Brazil)
	14*	Device color: • '0': Standard (black for most products) • '1': China UMS • '2': China ICBC • '3': PMS208c (Axis/India) • '4': FNB (South Africa) • '5': Gun metal • '6': Black • '7': Blue • '8': Red • '9': Black on Orange • 'A': Neon Green • 'B': Yellow • 'C': Black-Custom Geidea
	16	Range of Memory size configuration options. Permitted values for “M” are: “0”, “5”. • “0” = Standard (NAND-Flash 256MB/LPDDR2 SDRAM 128MB) • “1” = Reserved for Future Use (RFU): Standard/uSD • “2” = RFU: Extended (NAND-Flash 256MB/LPDDR2 SDRAM 256MB) • “3” = RFU: Extended/uSD

		• “4” = RFU: Standard/3SAM • “5” = Extended-PLUS (NAND-Flash 512MB/LPDDR2 SDRAM 512MB)
17		Extra Features: • “0”: None
19		HW ID for SoC silicon Revision. Permitted value: “B”
20		Range of Hardware ID Revision options. Permitted values for “R” are: “0”, “1”, “2”

Table 1, Hardware version variable positions

* Device color variable may include customer brand.

Examples of Customer branded devices

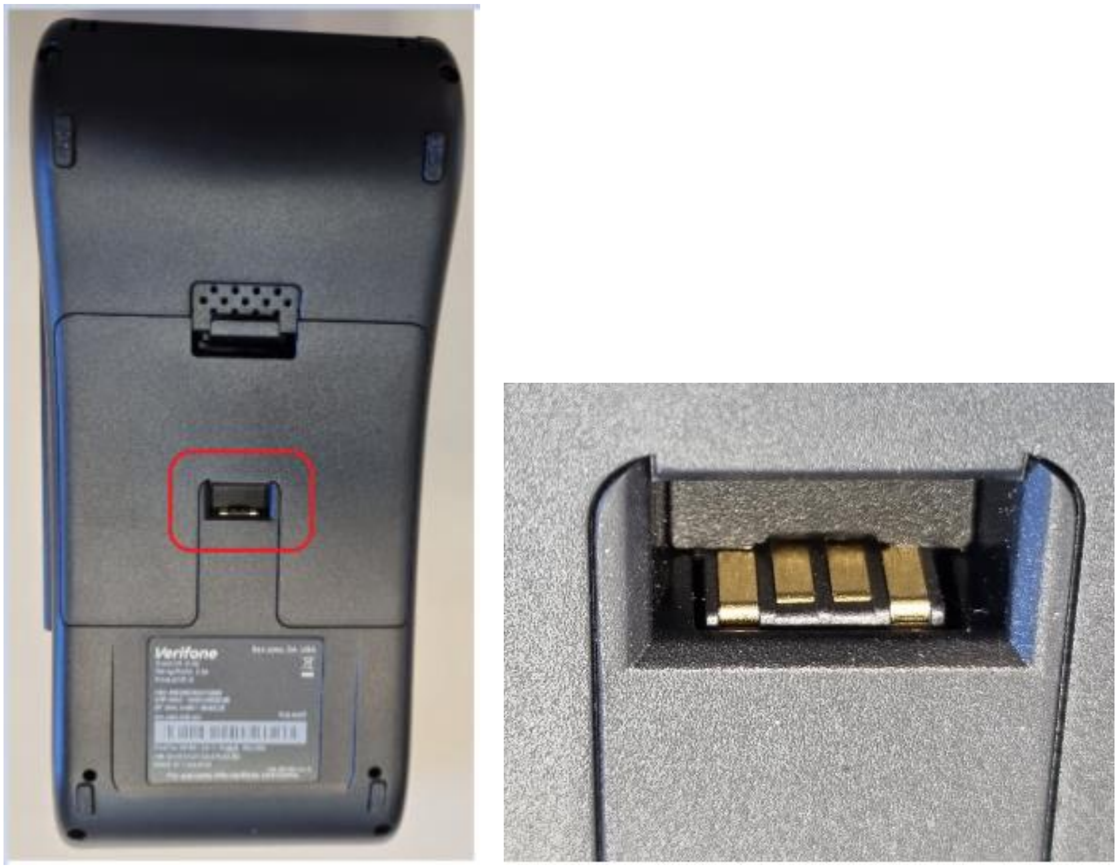


Model:V210 4G
Rating:5V ⎓ 2.2A
Product:V210
IMEI:862771040078498
WIFI MAC : 1848CAB62E23
BT MAC:A46011B5EF56
S/N:450-256-685

Prod No.:M183-124-11-EUA-6 Rev.A08
HW ID:H472-07-D2-070-00-B2
MADE IN THAILAND PL6 AI10
LBL183-001-04-A
For warranty info:verifone.com/terms

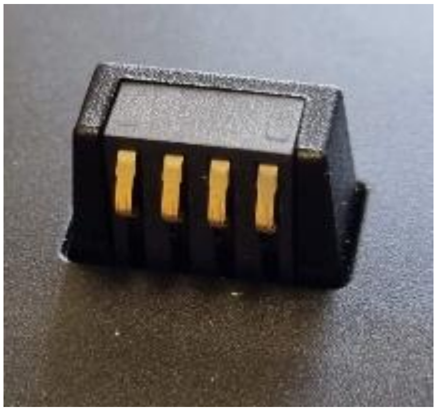
Figure 3, Example Hardware Identification

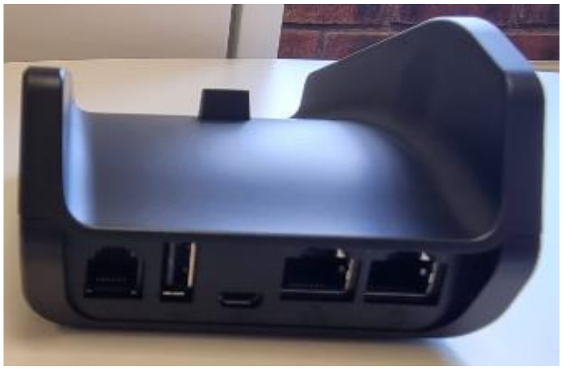
- The pictures below show the back of a V210 4G device docking port and the docking station, through which the charging and communication ports can be found.

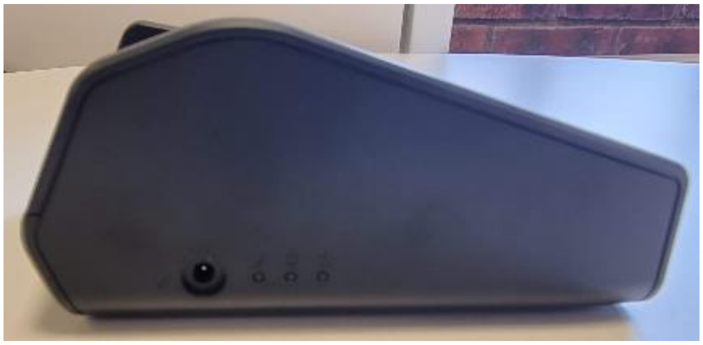


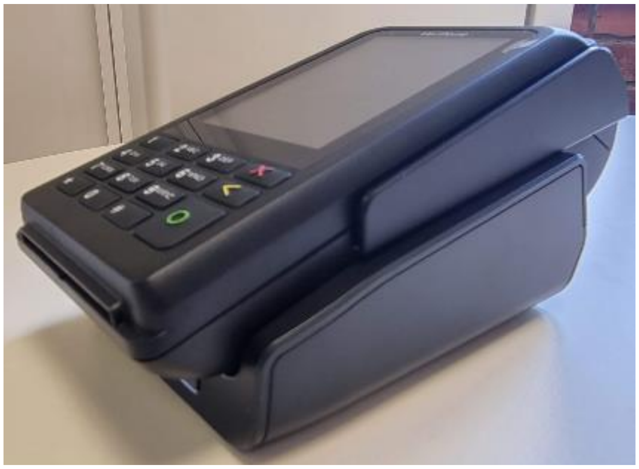
Example of a docking port on the back of a V210 4G series device

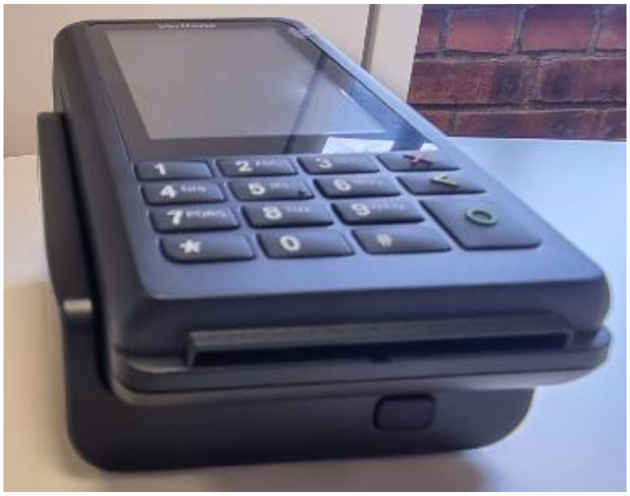
- Images of the docking station and docking port

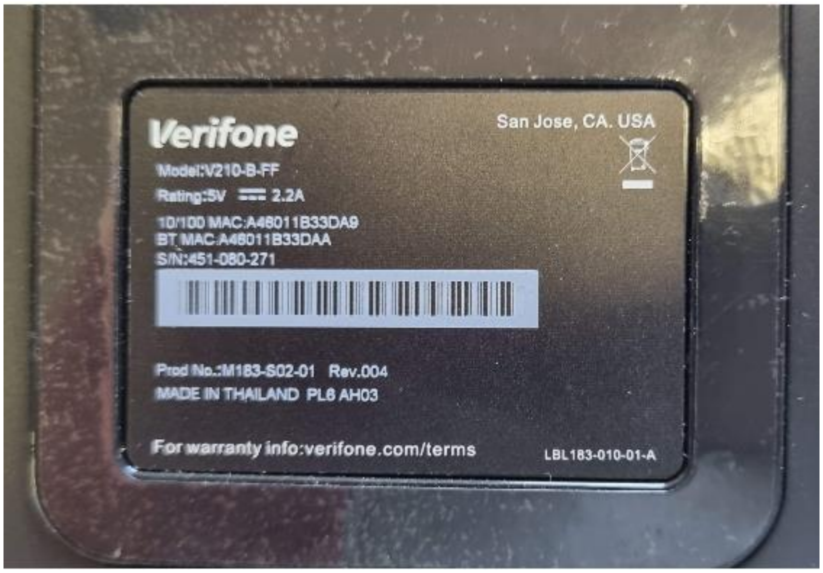




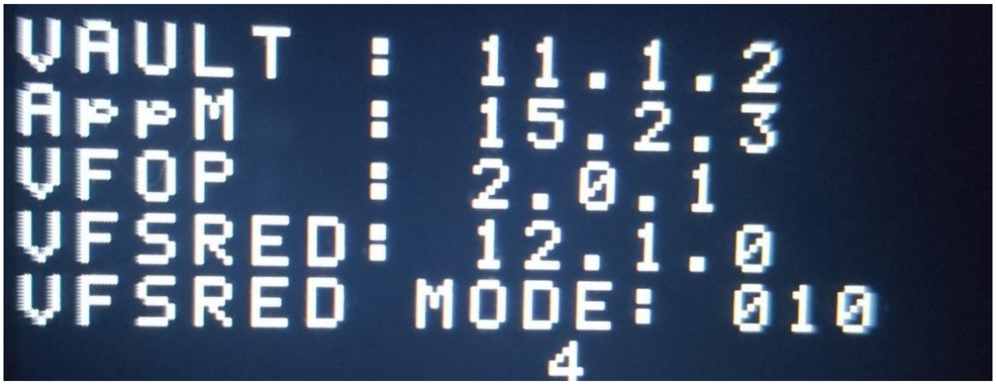







Verifone
San Jose, CA. USA
Model:V210-B-FF
Rating:5V ⎓ 2.2A
10/100 MAC:A46011B33DA9
BT MAC:A46011B33DAA
S/N:451-080-271
Prod No.:M183-S02-01 Rev.004
MADE IN THAILAND PL6 AH03
For warranty info:verifone.com/terms
LBL183-010-01-A

- Verifone Firmware is comprised of four Security Kernels, indicated below.
- For each of the four security kernels, the structure is X.x.x. “X” is the major digit that is updated whenever device payment security-related functionality is added or fixed. The middle “x” is updated whenever non-security related functions are added. The minor “x” digit is updated whenever non-security related bugs are fixed.
- The three last digits in VFSRED MODE version number show the VFSRED enablement status which is encoded according to Table 2.
- The firmware versions can be retrieved from the boot splash screen. Shortly after powering up, a splash screen displays the version number for the four security kernels; see Figure 5. You must be able to find these numbers on the list of Approved PIN Transaction Security (PTS) Devices (the major digits must match). If these numbers do not match, notify your service provider immediately.



```
VAULT  :  11.1.2
AppM   :  15.2.3
VFOP   :  2.0.1
VFSRED:  12.1.0
VFSRED MODE:  010
            4
```

Figure 5: Boot Splash Screen

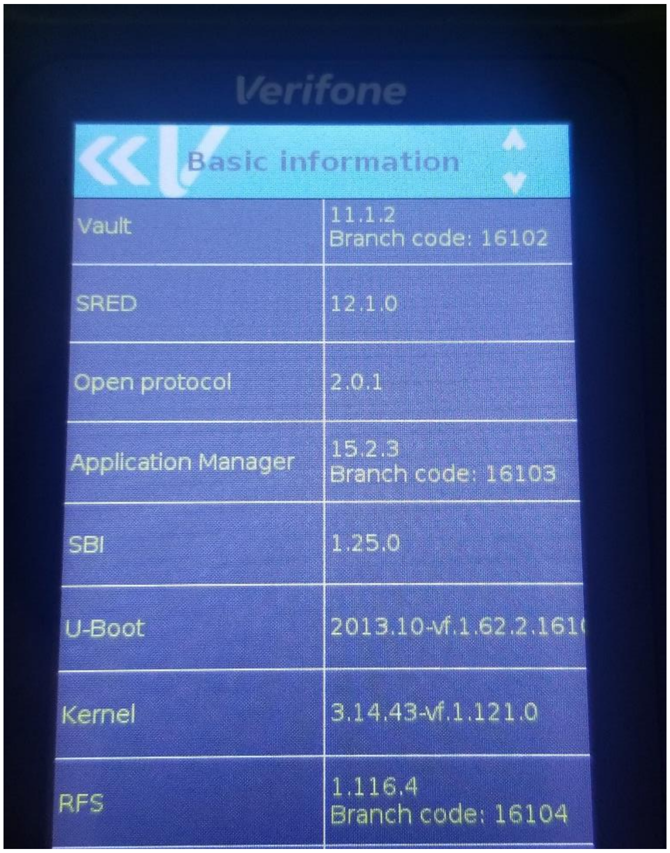
- The three last digits in VFSRED MODE version number show the VFSRED enablement status which is encoded according Table 2.

SRED Enablement			
	X	X	X
	1	2	3

1	VCL/ADE encryption: • 0 = VCL and ADE are disabled • 1 = ADE is enabled • 2 = VCL is enabled • 3 = ADE and VCL are enabled
2	ATOS Encryption: • 0 = ATOS is disabled • 1 = ATOS is enabled
3	Voltage encryption: • 0 = Voltage is disabled • 1 = Voltage is enabled

Table 2, SRED Enablement

- In addition, the detailed information about the security kernel versions can be shown on request from the "Basic information" panel in System Mode. To view the security kernel versions, login in System mode and select "Home > Information > Basic information" panel. Scroll through the screen and locate the four kernels; see Figure 6.
- Security kernels are:
  - Vault
  - SRED (equivalent to VFSRED in boot splash screen)
  - Open Protocol (equivalent to VFOP in boot splash screen)
  - Application Manager (equivalent to AppM in boot splash screen)



Basic information

Vault	11.1.2 Branch code: 16102
SRED	12.1.0
Open protocol	2.0.1
Application Manager	15.2.3 Branch code: 16103
SBI	1.25.0
U-Boot	2013.10-vf.1.62.2.161
Kernel	3.14.43-vf.1.121.0
RFS	1.116.4 Branch code: 16104

Figure 6, An example of Basic Information panel

INSTALLATION AND USER GUIDANCE

INITIAL INSPECTION

1) Carefully inspect the shipping carton and its contents for possible tampering or damage.
2) Validate the authenticity of the sender and the shipment by verifying the shipping tracking number, device serial number and other information located on the product order paperwork and the Advanced Shipping Notification (ASN). The HW and FW version numbers can be authenticated by reference to the Identification section of this document.
3) Remove the V210 unit from the shipping carton.
4) Remove any protective plastic wrap and place the unit on a table or countertop.
5) Remove the clear protective film from the display.
6) Inspect the terminal for possible tampering; see how to identify signs of tampering in

section Periodic Inspection.

7) Save the shipping carton and packing material for future repacking or moving the device.

INSTALLATION

- Configuration of the terminal must be performed prior to installation and use. The administrators should setup the maintenance user prior to installation and use.
- Prior to usage and deployment, familiarize yourself with the [R5] V210 Installation Guide (DOC183_003_EN_A01_V210_Installation_Guide). This guide provides information on verifying terminal equipment, usage, safety, security, environmental requirements, and troubleshooting steps if needed.
- The terminal contains no user serviceable parts. All repairs must be referred to an authorized repair facility. Disassembly will result in tampering the device.

ENVIRONMENTAL CONDITIONS

- The following are the temperature and humidity specifications of the V210:
  - Battery voltage: 3V
  - Operating temperature: -10º C to +55º C (14° to 131° F)
  - Storage temperature: -25° C to +65° C (-13° to 149° F)
  - Relative humidity: 5% to 90% (RH non-condensing)

- Subjecting the V210 to extreme environmental conditions will result in tamper events. Any temperatures above 105 ºC (± 5 degrees) or below -40 ºC (± 5 degrees) will result in a tamper condition. Additionally, should the battery voltage drift outside of the range of 1V (± 0.05V) VDC to 1.81V VDC (-0.18V to +0.2V), the unit will tamper as well.

COMMUNICATIONS AND SECURITY PROTOCOLS

- The V210 terminal supports the communications, methods, and protocols listed below. Use of any method not listed here invalidates the device PCI PTS approval.
- The following interfaces are available in the device:
  - USB-C (UART/RS232)

  - Bluetooth and Bluetooth Low Energy v4.2
  - Wi-Fi
  - Ethernet (through USB-C port)
  - Cellular (Cat-M1, 4G LTE Cat1)
  - 2G (for Cat-M1, or 4G LTE Cat1, fall back)
- The following protocols and services are supported by the device via the docking station:
  - TLS/SSL
  - Ethernet over USB
  - SFTP, SSH, PPP
  - DHCP, DNS, OCSP
  - ICMP, TCP, IP, UDP
  - PPP
- The security guidance described in this Security Policy and in [R7] V/OS IP Stack Security Guidance Users Guide specifies how protocols and services must be used/configured for each interface that is available on the device.
- It should be noted that not all the available functions offered by the V210 may be used for payment-based applications. Also, care must be used to ensure that each function is used in a manner compliant with PCI PTS POI requirements as all modes are not necessarily compliant.
- Within the V210, the default configuration for all communication interfaces is that they are disabled and not receiving. It is only when the operating system or application initiates a connection (acting as a client) that a port is opened, and the communication stack is activated.

CONFIGURATION SETTINGS

- The device is functional when received by the merchant or acquirer. No security sensitive configuration settings are necessary to be modified by the end user to meet security requirements.
- Only the configurations listed in the security policy are supported for these interfaces.
  - The information provided in SSL GUIDANCE must be followed.
  - All encryption algorithms, key lengths, and encryption strengths must be used in accordance with the ALGORITHMS SUPPORTED section of this document.

  - PTS approval is only valid for the platform containing the IP and link layer, the IP protocols, the security protocols, and the IP services, as provided by the vendor, and when used in accordance with the guidance supplied in this document.
  - Keys must not be shared between security protocols.

UNATTENDED INSTALLATION

- Not applicable.

HANDHELD DEVICES

- The V210 is an integrated handheld device. When the V210 is used in a Mobile-POS use case scenario connected to a mobile phone or tablet via Bluetooth / BLE 4.2 or Wi-Fi, the SRED data-account encryption functions must be enabled and enforced, otherwise it will invalidate the PCI-PTS approval for this device.

OPERATION AND MAINTENANCE

PERIODIC INSPECTION

- Inspect the terminal and docking station for possible tampering after receipt, during installation and periodically. Signs of tampering include:
  - Wires protruding out of the device
  - Foreign objects inserted into the smart card slot or mag stripe slot
  - Alterations of device stickers or labels
  - Signs of damage to the tamper evident labels
  - Tamper message on the device display; see Figure 9.
- In addition, administrators or site managers should:
  - Implement a procedure that checks the terminal serial number every time the device is started or powered on to ensure the device has not been replaced. If the device has been replaced, cease using the terminal and notify your Verifone customer relations manager.
  - Visually inspect the terminal and docking station daily to ensure there are no foreign

objects present in the smartcard slot or other ports. Ensure there are no wires emanating from the smartcard slot.

- Develop a breach response plan. This identifies the steps to take if a suspected breach occurs and as well as who will perform each step. The plan needs to include isolation of your payment systems and a list of all personnel who need to be notified. These personnel include your local law enforcement, acquiring bank, processor, security assessor, as well as your payment system vendor.
- Track each instance of replaced terminals or docking stations within the store. Whether from the in-store inventory, by a repair technician or with terminals shipped into the store.
- If any device is found in tamper state, please remove it from service immediately, keep it available for potential forensics investigation, and notify your company security officer and your local Verifone representative or service provider. For contacting Verifone, please see section “Verifone Service and Support” in [R5] V210 Installation Guide (DOC183_003_EN_A01_V210_Installation_Guide).

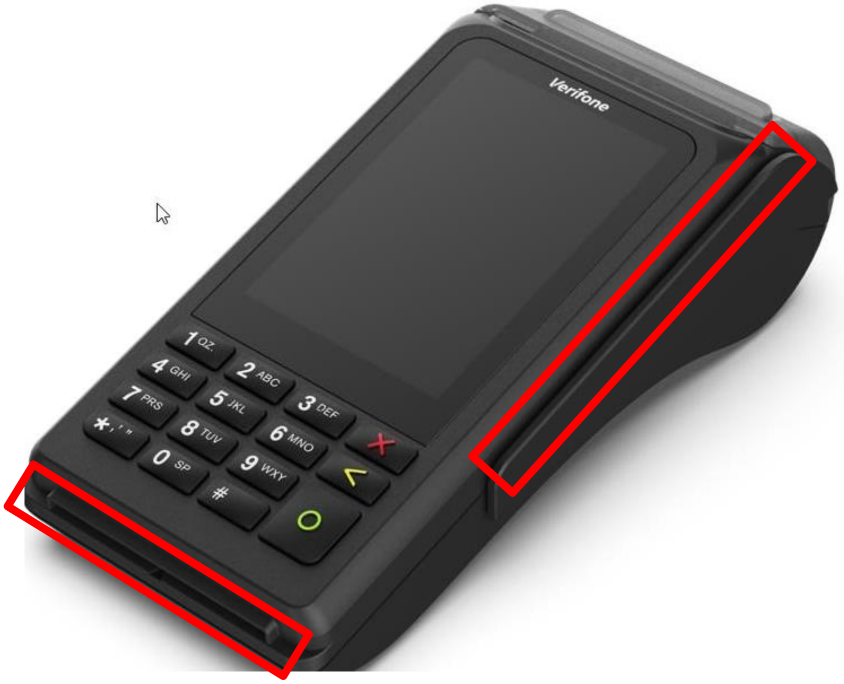


Figure 7: Mag stripe slot and smartcard slot

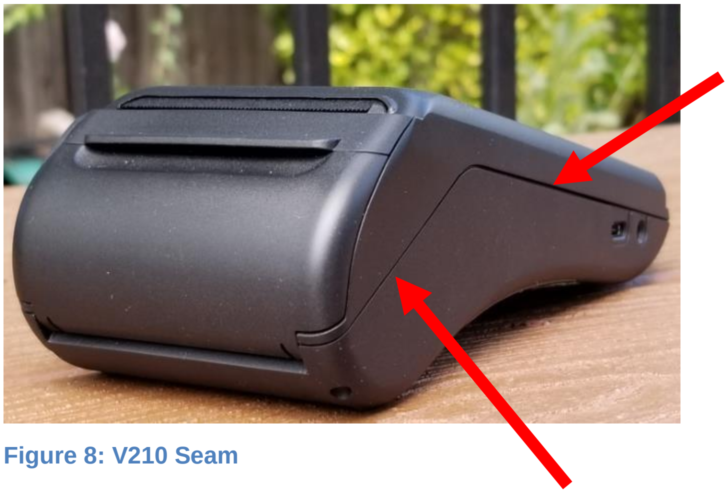


Figure 8: V210 Seam

SELF-TEST

- V210 terminals employ a self-test to confirm firmware integrity and reinitialize memory. The self-test is performed:
  - When the unit powers
  - When the unit is rebooted
  - At least once every 24 hours
  - Upon demand, like going into System Mode and causing the terminal to reboot.
- The self-test option can also be manually invoked via access to System Mode.
- The following components are checked during self-test:
  - Integrity of the TMK (Terminal Master Key)
  - Integrity of the other key files
  - Tamper detection system
  - VeriShield certificate tree
  - Firmware
- If a self-test fails, the V210 limits its functionality based on the severity of the issue discovered. Device response ranges from partial disablement of applications to non-functionality. In all cases PIN-processing is disabled.

ROLES AND RESPONSIBILITIES

- This document is useful for the following users:
  - Technicians deploying V210 series terminals to end user sites performing specific

tasks required to deploy a new V210 terminal into the field, such as:

    - Configuring terminals
    - Downloading application software
    - Testing terminals prior to deployment

  - Administrators or site managers performing administrative and on-site duties, such as:
    - Changing passwords
    - Performing routine tests and terminal maintenance
    - Configuring terminals for remote diagnostics and downloads

PASSWORDS

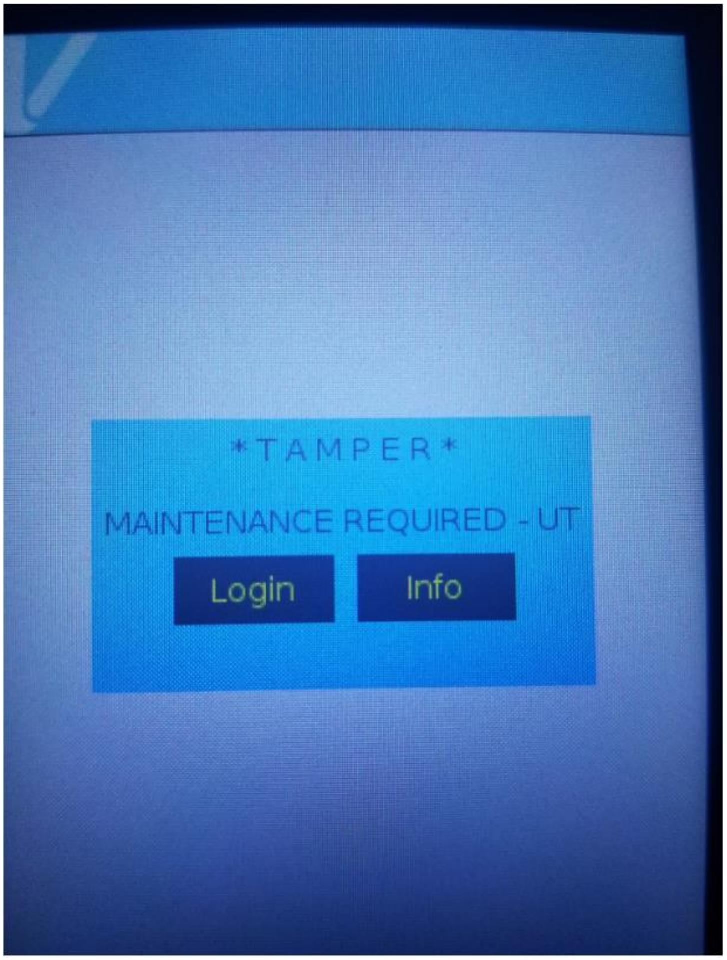
- Passwords used for entering in System Mode and entering sensitive services (key loading) are pre-expired and must be changed upon first use. No sensitive functions are possible until the pre-expired passwords are changed to new and unique values. Changing the passwords back to the default values is not possible. These passwords must be at least 7 decimal characters (0-9) in length.

CERTIFICATES

- Certificates are used to authenticate the Firmware, and to authenticate & establish ownership of the PED to a specific vendor-merchant. For example, once the PED is loaded with a specific vendor-merchant's certificate, that terminal cannot be loaded and used by another vendor.

TAMPER RESPONSE

- Security mechanisms employed within the terminal can detect physical tampering and trigger a tamper event. This causes the terminal to cease performing transactions and indicates that it has been tampered on the display; see Figure 9.



TAMPER

MAINTENANCE REQUIRED - UT

Figure 9, Tamper message on the terminal display

CARDHOLDER PIN ENTRY

The V210 series terminals are handover devices. Always exercise extreme caution when conducting transactions. During PIN entry, the merchant should:

- Hand the terminal directly to the cardholder
- Instruct the cardholder to orient the terminal and themselves to prevent PIN spying by others and any cameras mounted in the vicinity

Verifone also recommends instructing the merchants and installers to create a safe PIN-entry area using a combination of techniques including but not limited to:

- Positioning signage and literature at the point of sale, and in the queue area
- Positioning in-store cameras such that PIN entry is NOT visible
- Arranging the queue to physically isolate the cardholder to ensure privacy during PIN entry.

PATCHING AND UPDATING

- Updates and/or patches to the operating system can be installed in the device.
- Updates/patches are RSA certificate authenticated. If the signature of the updates cannot be authenticated, the update/patch is rejected and not installed.
- Local update functions are accessible within System Mode and are supported via USB Memory Drive.
- Remote update functions are supported via:
    - VHQ (Verifone's terminal management system)
    - Applications can use the software installation and secure communication APIs supported in the operating system.
- For the secure operation of the device, it is recommended to use the latest versions of the released software.

DECOMMISSIONING

- Before removing the device from service permanently or for repairs, all sensitive data must be erased. Sensitive data includes credit card data and all encryption keys inclusive of ALL Private, PIN, and data encryption keys.
- This can be done by disassembling the device in order to force a tamper condition, so all sensitive data will be erased automatically. After performing this operation, turn on the terminal and verify that the unit is in tamper state; see Figure 9.

THEFT AND LOSS

- Should the device be stolen or lost, the police and/or local security services should be contacted as appropriate.
- Additionally, the local Verifone office and/or third-party service provider should be notified.

REMOVAL DETECTION

- Not applicable.

SECURITY

SOFTWARE DEVELOPMENT GUIDANCE

- Applications must be designed and implemented in accordance with the PA-DSS requirements document entitled, [R11] PA-DSS Program Guide v3.2.
- When developing IP capable payment-based applications, developers must follow the guidance listed in the following documents:
  - This Security Policy
  - [R6] V/OS Programmer's Manual (VPN – DOC00501)
  - [R7] V/OS IP Stack Security Guidance Users Guide
  - [R10] VeriShield File Signing Overview
- All referenced best practices regarding coding practices and device configurations must be followed.
- Transaction data must be cleared as soon as the transaction is completed, including but not limited to working registers and buffers.
- Allowable application behaviors:
  - Writing to the display
  - Fetching keypad entries
  - Requesting an encrypted PIN block
- Forbidden application behaviors:
  - Changing PIN entry retry limit
  - Attempting to alter PIN entry time-out.
    - PIN entry time-outs are set and enforced by the OS. The application is not capable of altering them.
    - PIN Entry time-outs are set to 30 seconds without key presses or 300 seconds with key presses.
  - Modifying a key
  - Generating a subordinate certificate
  - Executing another application
  - Encrypting arbitrary data

SSL

- TLS 1.2 should be used. SSL is supported but this protocol is inherently weak and should be removed unless required on an interim basis to facilitate interoperability as part of a migration plan. For SSL 3, or older versions of TLS, if supported, all cipher suites using single DES or RC4 must be removed.
- It is strongly advised to use TLS/SSL with mutual authentication enabled to protect the communications over a network connection.

BLUETOOTH

- The IP Stack supports Bluetooth BR/EDR (Classic), Bluetooth Low Energy v4.2 and transmit only beacons (iBeacon and EddyStone).
- The Bluetooth interface is configured by the Operating System to enforce encryption and use PCI-PTS approved secure pairing options only. No security-sensitive configuration settings are necessary to be modified by the end user to meet the security requirements.
- The Bluetooth Low Energy interface is configured to enforce encryption. This encryption is in addition to any other encryption the data may have undergone. This implies that the configuration of the GATT server must enable authenticated signed reads and writes of Characteristics, so that the communication will be only possible with paired clients.
- Beacons are transmitting only, and it cannot be used to transmit sensitive data. Over the Air provisioning is not supported.
- Follow the instructions below to mitigate attacks on the Bluetooth interface:
    - Make sure that the terminal has the latest software updates and security patches.
    - Make sure that the peer device connected via Bluetooth, e.g. computer or mobile device, periodically receive software updates and security patches.
    - Perform Bluetooth device pairing as infrequently as possible and ideally in a physically secure area where attackers cannot observe passkey entry and eavesdrop on Bluetooth pairing-related communications.
    - Provide application layer security on top of Bluetooth to encrypt the data as a generic countermeasure to mitigate attacks to Bluetooth interface.
- Detailed information regarding the security capabilities of Bluetooth and recommendations

to organizations employing Bluetooth wireless technologies on securing them effectively can be found in [R12] NIST Special Publication 800-121 - Guide to Bluetooth Security.

WI-FI

- The IP Stack provides the following Wi-Fi main security configurations:
  - WPA (Wi-Fi Protected Access)
  - WPA 2 (Wi-Fi Protected Access 2)
- WEP is not supported.
- It is recommended that WPA2 Personal mode be used with a minimum 13-character random passphrase and AES encryption.
- In addition to the used Wi-Fi secure protocol (WPA or WPA2), the communication should be secured using a secure protocol such as TLS 1.2.
- Wireless encryption keys must be changed from default at installation, changed anytime anyone with knowledge of the keys leaves your company or changes positions and at least every 90 days.
- Default passwords/passphrases on routers/access points must be changed at installation, changed anytime anyone with knowledge of the keys leaves your company or changes positions and at least every 90 days.
- For more information, please refer to [R13] Information Supplement: PCI Wireless Guidelines.

SIGNING

- VeriShield FST (File Signing Tool) manages the generation and signing of device certificates. See DevNet and [R10] VeriShield File Signing Overview for more information on signing tool implementation.
- V210 terminals employ a security architecture called VeriShield Retain, which has both physical and logical components. The logical security component, called File Authentication (FA), is part of the terminal’s operating system software.
- File Authentication is a secured process for authenticating files using digital signatures, cryptographic keys, and digital certificates. This process enables the sponsor of a V210 terminal to logically secure access to the terminal by controlling who is authorized to download applications or firmware updates files to the terminal. It proves and verifies the

file's origin, sender's identity, and the integrity of the file's information. If any of these three items are not verified, then the download is rejected.

- Only application codes that have been authorized for release should be signed and released to the field. The signing must occur under dual control and split knowledge.

ACCOUNT DATA PROTECTION

- The encryption of PAN data is automatic and transparent to your application – there are no added API calls needed.
- The device supports account data protection using format-preserving encryption (FPE) revised FF2.1 method. The pass-through of clear-text account data is supported using whitelisting technique (BIN table).
- In addition, the device supports account data encryption operations using TDEA DUKPT algorithm (ADE and ATOS Poseidon ZVT Security), AES DUKPT (VCL) and VISA DSP.
- SRED functionality is enabled as part of the key loading process during manufacturing. Once SRED is enabled, it cannot be disabled.

ALGORITHMS SUPPORTED

- Only use acceptable cryptographic algorithms listed in [R4] SP800-57 Part 1: Recommendations for Key Management. The cryptographic strength must be at least 112 bits.
- The device supports the following algorithms:
  - TDEA (128, 192 bits)
  - AES (128, 192, 256 bits)
  - RSA (2048 bits)
  - ECDSA (256, 384, 521 bits)
  - SHA-256, SHA-384, SHA-512
- Although other cryptographic algorithms may be supported by the terminal, they may not be used for payment-based applications.
- PTS approval is only valid for the platform containing the IP and link layer, the IP protocols, the security protocols, and the IP services, as provided by the vendor and when used in accordance with the guidance supplied in this document.

- Keys may NOT be shared between security protocols.

KEY MANAGEMENT

- The device supports the following key management schemes:
  - Master Key / Session Key (TDEA)
  - DUKPT (TDEA and AES)
- Employing key management schemes that do not comply with PCI PTS with PCI payments will invalidate the PCI PTS approval for this POI.
- Fixed key is not supported by the device for account-data and PIN encipherment for PCI-brand transactions.
- The device supports the TR-34 One Pass method. The Two Pass method is not supported.
- For devices to be deployed in countries requiring Common.SECC certification, the use of fixed key or master/session key management schemes and PIN block format 0 for PIN encryption must be avoided and unique keys per transaction or the use of PIN block format 1 (random included) shall be used instead.
- The following table lists all supported key management schemes. For more information, refer to [R9] 2.0 Encryption Services Organization Key Management Procedures.

Key Name	Purpose/ Usage	Algorithm	Size (Bits)	Form Factor Loaded to Device In	Number of Available Key Slots (Registers)
KLK (Key Loading Key)	To load Master keys encrypted from HSM.	TDEA	128 or 192	Plaintext from key injection device	1
DUKPT (PIN and MAC)	PIN encryption and message authentication.	TDEA DUKPT	128	Plaintext from key injection device or remotely loaded (VRK)	3 sets of keys
AES DUKPT (PIN, VCL)	PIN encryption, message authentication, and data encryption.	AES DUKPT	128, 192, or 256	Plaintext from key injection device or remotely loaded (VRK)	3 sets of keys

Terminal Master Key (TMK)	Encryption of working keys (PEK, MAC) for down-line transmission to the device	TDEA	128 or 192	Plaintext from key injection device, encrypted under KLK, or remotely loaded (VRK)	10
PIN Encryption Key (PEK)	PIN encipherment for online PIN	TDEA	128 or 192	Encrypted under Terminal Master Key (TMK)	1
MAC Key	Message authentication	TDEA	128	Encrypted under Terminal Master Key (TMK)	1
Data Key	Account balance decryption	TDEA	128	Encrypted under Terminal Master Key (TMK)	1
Fixed MAC Key	Message authentication	TDEA	128	Plaintext from key injection device, encrypted under KLK, or remotely loaded (VRK)	10
Account Data Encryption Key (ADE)	To encrypt account data and for message authentication (using the encryption and MAC key variants as generated per standard DUKPT)	TDEA DUKPT	128	Plaintext from key injection device or remotely loaded (VRK)	10
ATOS Poseidon Keys	PIN Encryption, message authentication, bitmap encryption and end-to-end encryption per ATOS Poseidon scheme	TDEA	128	Plaintext from key injection device or remotely loaded (VRK)	1
VCL Key	Keys for Format Preserving Encryption of card data per Verifone VCL scheme	AES	128	Two plaintext components on MSR cards	1
Application Signer	Used by customer to sign Applications to install to device.	RSA 2048 with SHA-256	2048	X509 public key certificate	1

KEY LOADING

- The terminal does not support manual cryptographic key entry. Key injection and management equipment must be managed in a secure manner to minimize the opportunity for compromise in accordance with items [R1], [R2], and [R3] in References.
- Physical keys, authorization codes, passwords, and other credentials must be managed under dual control and split knowledge so that no one person can use two credentials simultaneously.
- Key management security objectives must be in compliance with PCI PIN Transaction Security requirements.

KEY REPLACEMENT

- Key replacement must be performed upon any known or suspected compromise of any cryptographic or sensitive information, and whenever the time deemed feasible to determine the key by exhaustive attack elapses, as defined in NIST SP 800-57-1.

ANNEX

RELATED DOCUMENTATION

[R1] ANSI x9.24 Part 1:2017, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques

[R2] ANSI x9.24 Part 2:2017, Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys

[R3] X9 TR-31:2018, Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms

[R4] SP800-57 Part 1: Recommendation for Key Management

[R5] Verifone V210 Installation Guide (VPN – DOC474-003-EN-A)

[R6] V/OS Programmer’s Manual (VPN – DOC00501)

[R7] V/OS IP Stack Security Guidance Users Guide

[R8] Point of Interaction (POI) Modular Security Requirements v6.0 June 2020

[R9] 2.0 Encryption Services Organization Key Management Procedures

[R10] VeriShield File Signing Overview

[R11] PA-DSS Program Guide v3.2

[R12] NIST Special Publication 800-121 - Guide to Bluetooth Security

[R13] Information Supplement: PCI Wireless Guidelines

ACRONYMS

#:	Number
AES:	Advanced Encryption Standard
ANSI:	American National Standards Institute
API:	Application Programming Interface
BT	Bluetooth
DEA:	Data Encryption Algorithm
DUKPT:	Derived Unique Key Per Transaction
FIPS:	Federal Information Processing Standards
FA:	File Authentication
FST:	File Signing Tool
LCD:	Liquid Crystal Display
MAC:	Message Authentication Code
PA-DSS:	Payment Application Data Security Standard
PAN:	Personal Account Number
PCI:	Payment Card Industry
PED:	PIN Entry Device
PIN:	Personal Identification Number
POI:	Point of Interaction
PTS:	PIN Transaction Security
RH:	Relative Humidity
RSA:	Rivest Shamir Adleman

SHA:	Secure Hash Algorithm
SRED:	Secure Reading and Exchange of Data
TDEA:	Triple Data Encryption Algorithm
TMK:	Terminal Master Key
VPN:	Verifone Publication Number